CERT

Focus on Resiliency: A Process-Oriented Approach to Security

Rich Caralli James Stevens

Carnegie Mellon University Software Engineering Institute

32nd Annual CSI Conference & Exhibition

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Focus on Resiliency: A Process-Oriented Approach to Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
32nd Annual CSI Conference & Exhibition, held in Washington, D.C., on November 14-16, 2005.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**88**	

Agenda

About the SEI

Characterizing the problem

Security, resiliency, and risk

A process-oriented approach

Thinking about solutions

Conclusions and next steps

Questions

Software Engineering Institute -1

Federally Funded Research and Development Center; awarded to Carnegie Mellon University in 1984 based on competitive procurement

Sponsored by Office of the Under Secretary of Defense (Acquisition, Technology, & Logistics); contract administered by USAF Electronic Systems Center (ESC)

Offices in Arlington, VA, Huntsville AL, Pittsburgh, PA and Frankfurt, Germany

Software Engineering Institute -2

Mission is to provide leadership in software engineering and to transition new software engineering technology

Encouraged to support industry in pre-competitive technology research and development and in technology transition activities

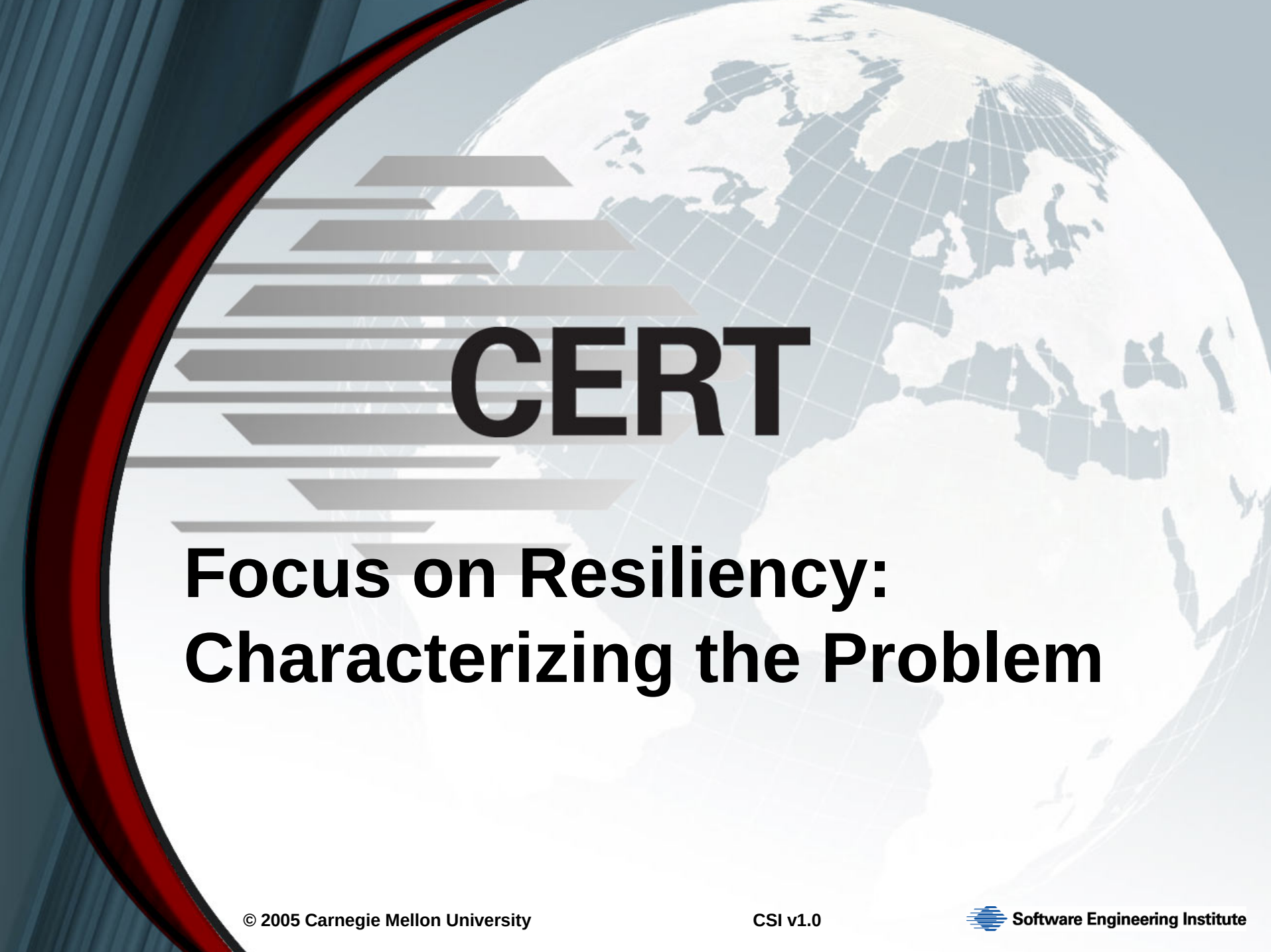
SEI Technical Programs

Product Line Systems

Dynamic Systems

Software Engineering Process Management

Networked Systems Survivability or CERT



Focus on Resiliency: Characterizing the Problem

What is the problem?

Is your organization's security capability sufficient to identify and manage risks that result from

- failed internal processes
- inadvertent or deliberate actions of people
- problems with systems and technology
- external events

Why does it matter?

Organizations must focus their limited resources on identifying and managing the risks that have the most potential to

- disrupt its core business drivers
- impede the survivability of its mission

Lessons from OCTAVE℠

- Organizational focus improves information security activities
- Operational unit-driven risk assessment more meaningful

- Organization often impedes progress of operational units
- Sustained organization-wide improvement still elusive
- Risk assessment not equal to active risk management

Operationally Critical Threat, Asset, and Vulnerability Evaluation

Recent case history -1

Poorly planned and organized security function and roles/responsibilities

No active involvement of business units

No information asset management

Funding model reactive, not strategic

Regulatory drivers not a sufficient driver for success

Recent case history -2

Attaining and sustaining security success difficult

Security is a technical function

Frequent collisions between operational units and organization on security strategy

Searching for magic bullet – ITIL, COBIT, etc.

“Can someone else do this for us?”

Fieldwork conclusions -1

Security is often an end-state or “goal”

Security activities are predominantly technical

Technical leadership drives security program

Senior-level sponsorship, planning, and funding lacking

Organizational context of security ignored

Fieldwork conclusions -2

Lack of collaboration across enterprise

Failure to recognize risk as the basis for security activities

Best practices substitute for active management

Quick fix preferred over developing competency

Security isolated from operational risk management

A new operational environment -1

No operational boundaries

Pervasiveness of technology

Expanding and rapidly changing risk profile

High dependency on upstream partners

Successes are short-lived

Skills have shorter longevity

Less resources, more demands

A new operational environment -2

Increasing regulatory requirements

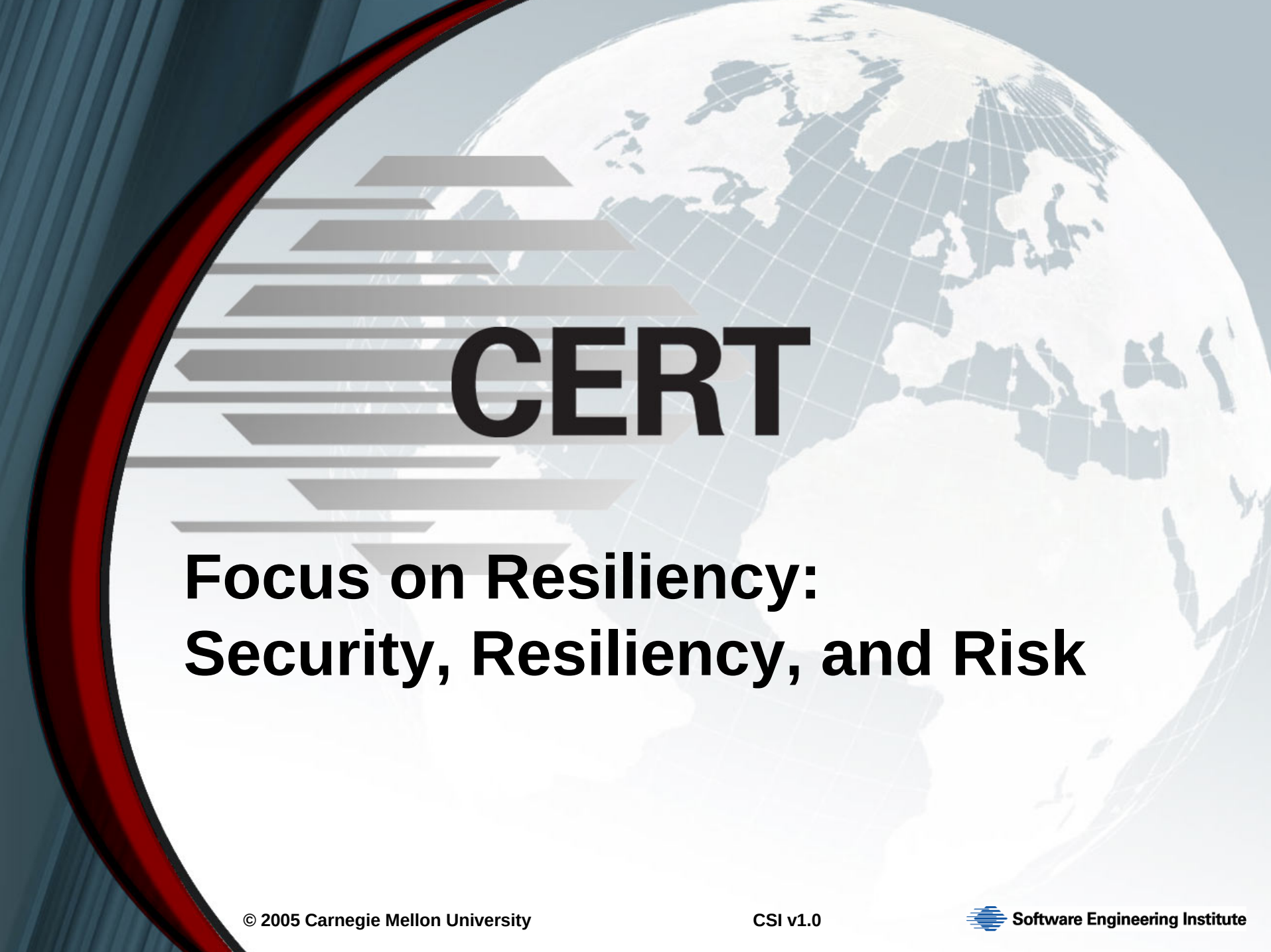
Criticality of data and information

Distributed workforce

Heightened threat level and increasing uncertainty

Insurance costs

Reliance on third-parties



Focus on Resiliency: Security, Resiliency, and Risk

Back to basics

To make security a more effective activity in the organization, we must:

1. Re-define its role and contributions
2. Acknowledge risk as the driver
3. Position it as an enabler to resiliency
4. Manage it as a process that can be improved: PLAN→DO→CHECK→ACT

Redefining security -1

How do we view security in the organization?

From	To
▪ Technical issue	▪ Business issue
▪ Owned by IT	▪ Owned by organization
▪ Expense-driven	▪ Investment
▪ Practice-centric	▪ Process-centric
▪ Security & survivability	▪ Enterprise resiliency

Redefining security -2

How do we approach security in the organization?

From

- **Irregular**
- **Reactive**
- **Immeasurable**
- **Absolute**
- **AD-HOC and TACTICAL**

To

- **Systematic**
- **Adaptive**
- **Measured**
- **Adequate**
- **MANAGED and STRATEGIC**

Redefining security -3

How do we perform security in the organization?

From

- **Protective stance**
- **Monitoring**
- **Reacting to complexity and risk**
- **Rewarding individual heroics**

To

- **Enabling stance**
- **Sensing**
- **Adapting to complexity and risk**
- **Rewarding collaboration and process improvement**

Summary

Security is a business issue

Security is owned by the organization

Security is an investment

Security is an enterprise process that can be measured and managed

The goal of security is to contribute to attaining and sustaining enterprise resiliency

Resetting success criteria

C-level sponsorship and authority

Strategic planning

Achievable and measurable goals

Limited control and influence of IT

Organization-wide resources

Adequate and sustained funding

On-going process management

Operational risk management and resiliency focus

Back to basics

To make security a more effective activity in the organization, we must:

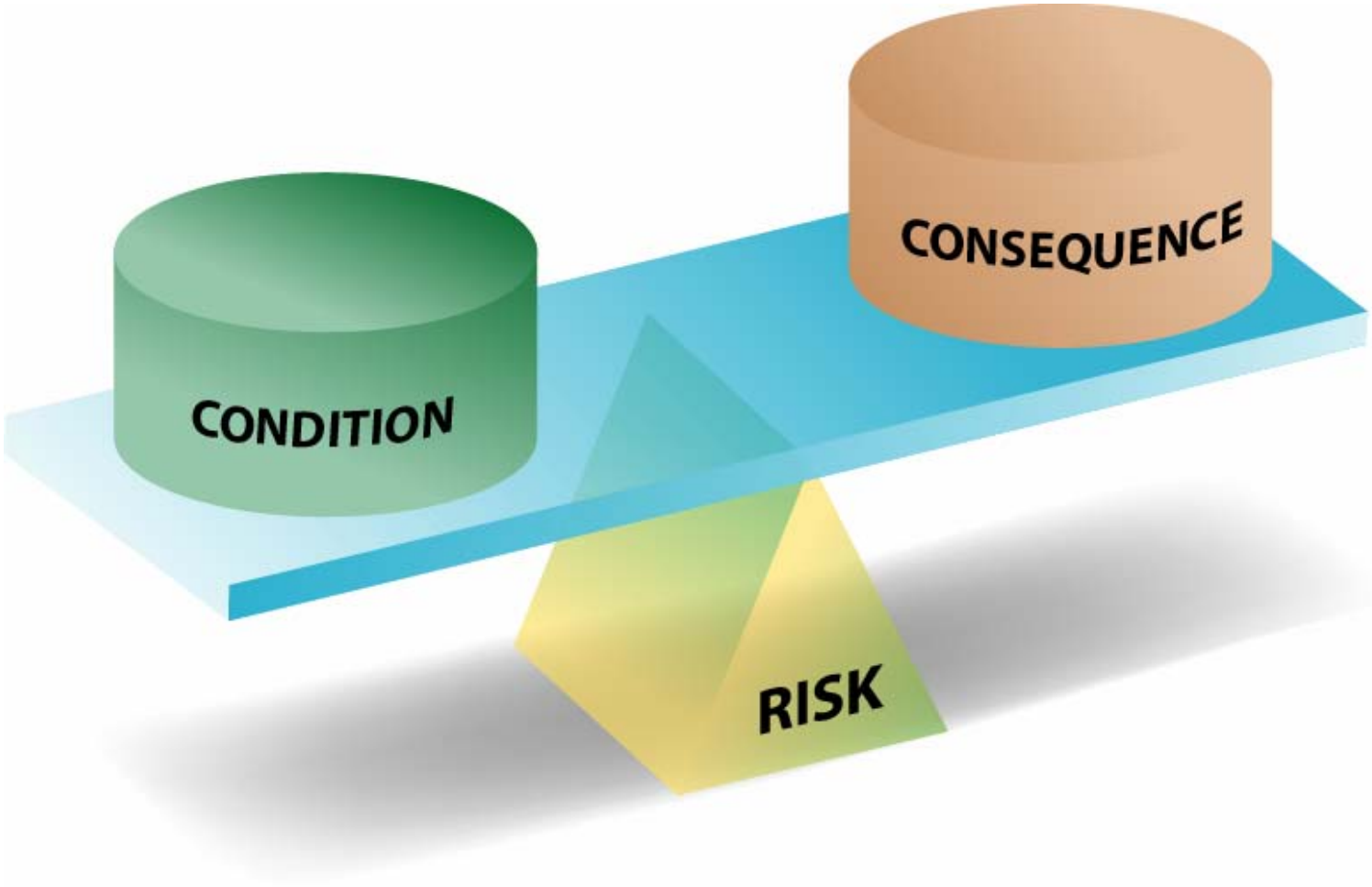
1. Re-define its role and contributions
2. Acknowledge risk as the driver
3. Position it as an enabler to resiliency
4. Manage it as a process that can be improved: PLAN→DO→CHECK→ACT

The rationale for security

Protect critical enterprise assets (information, technology, facilities, and people)

- Keep business processes are viable and mission-focused
- Minimize disruptions in achieving enterprise goals and mission
- Contribute to the management of operational risk and resiliency

The risk equation



Operational risk

A form of hazard risk affecting day-to-day business operations

The potential failure to achieve mission objectives

Must be managed to ensure the organization's resiliency

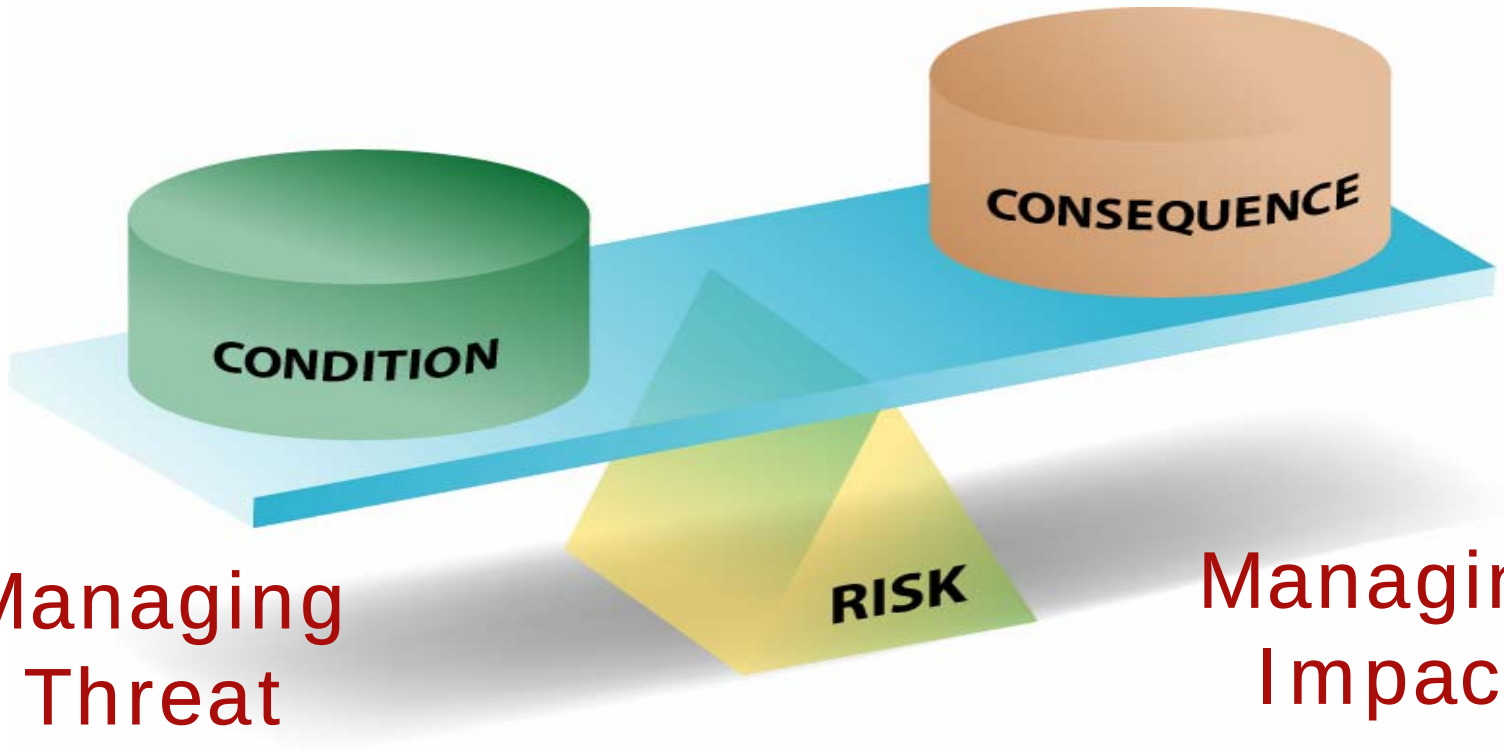
Operational risk management

- A new operational environment brings a need for sustainable improvement in managing operational risk
- Security management is a significant component of managing operational risk

"Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events."

--Basel II Capital Accords

ORM requires balance



Managing ORM

Two choices:

1. Manage threat by reducing the likelihood of the condition occurring
2. Manage impact by reducing potential impact and/or ensuring the organization can handle the result of a realized risk

Enterprise resiliency requires BOTH.

Back to basics

To make security a more effective activity in the organization, we must:

1. Re-define its role and contributions
2. Acknowledge risk as the driver
3. Position it as an enabler to resiliency
4. Manage it as a process that can be improved: PLAN→DO→CHECK→ACT

What is enterprise resiliency?

The competency and capacity of the enterprise to adapt to changing risk environments.

- Emerging threats to critical assets
- Changes in business environment
- Changes in social, geographical, and political environments
- Disruptions in upstream and downstream value chain
- Insider threat and fraud
- Natural disasters

Notable definitions of resiliency

Withstand systemic discontinuities and adapt to new risk environments [Booz-Allen04]

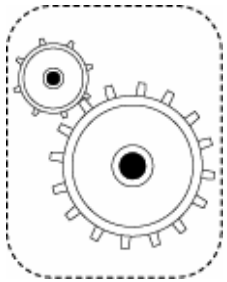
Be sensing, agile, networked, prepared [Booz-Allen04]

Dynamically reinvent business models and strategies as circumstances change [HBR05]

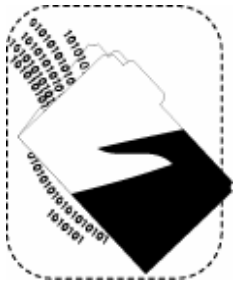
Have the capacity to change before the case for change becomes desperately obvious [HBR05]

Focused on five objects

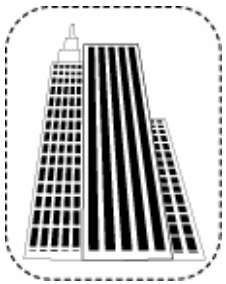
people



business processes



information



facilities

technology

People

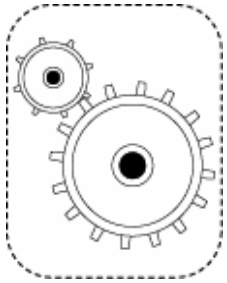
people

The human capital of the organization

Use the other objects of resiliency to ensure goal achievement

Disruptions to human resources often result in the failure of business processes to achieve their mission

Business processes



business processes

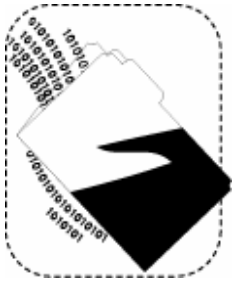
Most important resiliency object

The engine that propels the organization toward its mission

Each business process has its own mission that contributes to the larger mission

Interruptions in business processes are disruptive to the resiliency of the enterprise

Information



information

One of the most important assets of the organization

Business processes cannot operate effectively without access to information

Disruption of availability of information (either through modification, loss, or destruction) directly affects enterprise resiliency

Technology

technology

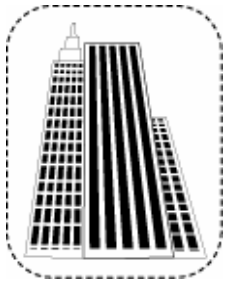
Directly supports the automation of critical business processes

Prominent factor in accomplishing mission

Pervasive across all functions of the organization

High exposure to risk that can affect the viability of other resiliency objects such as information and facilities

Facilities



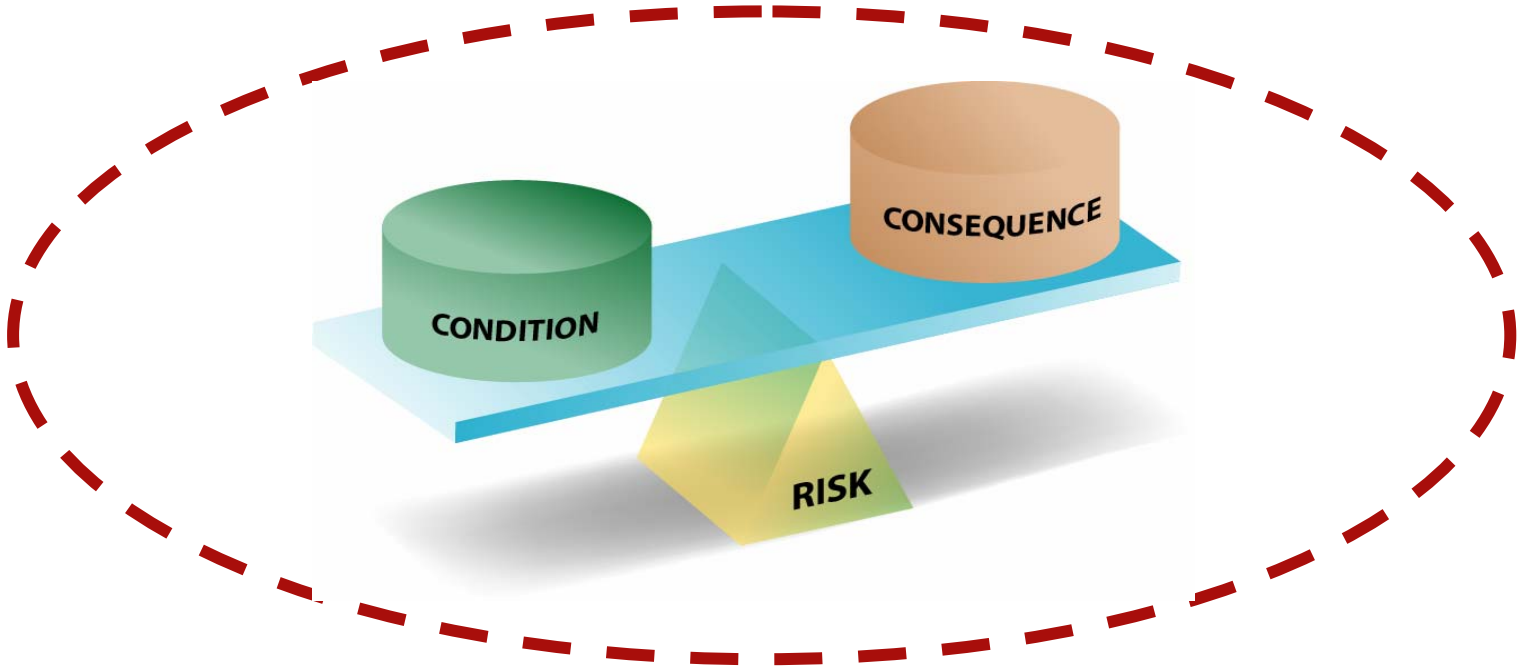
facilities

The physical places where other resiliency objects “live”

Provides direct support for business process achievement

Disruption to facilities often directly affects the other resiliency objects

Resiliency is a holistic approach

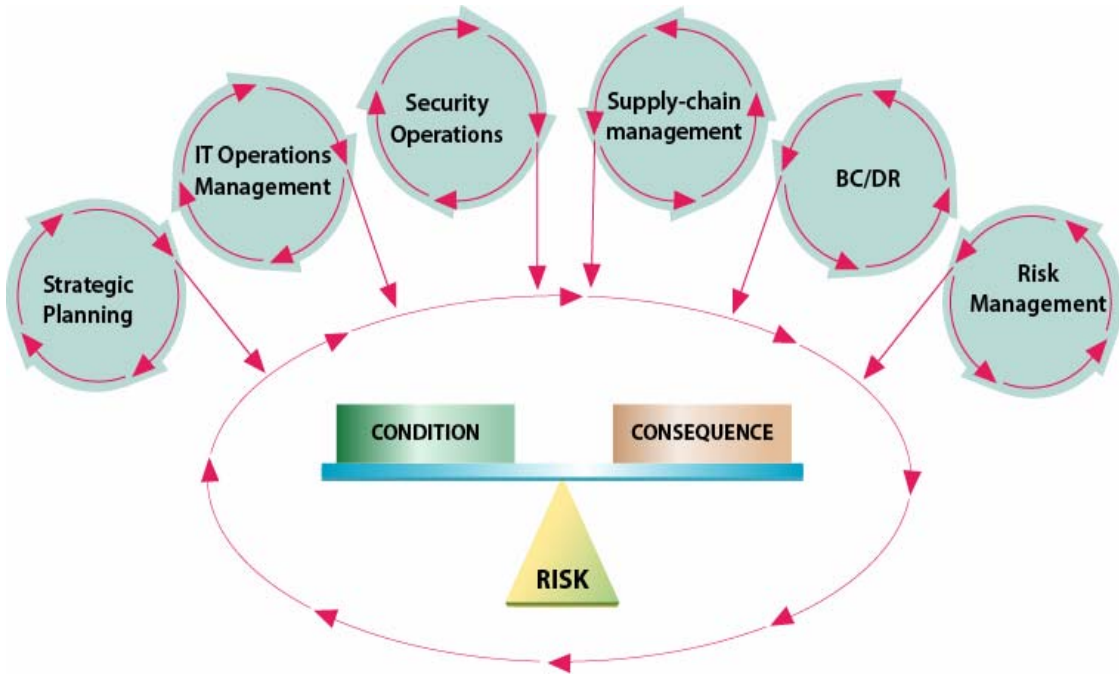


Managing both sides of the risk equation as a whole, in balance with organizational drivers and costs, to achieve a level of adequate resiliency.

Achieving resiliency is a challenge

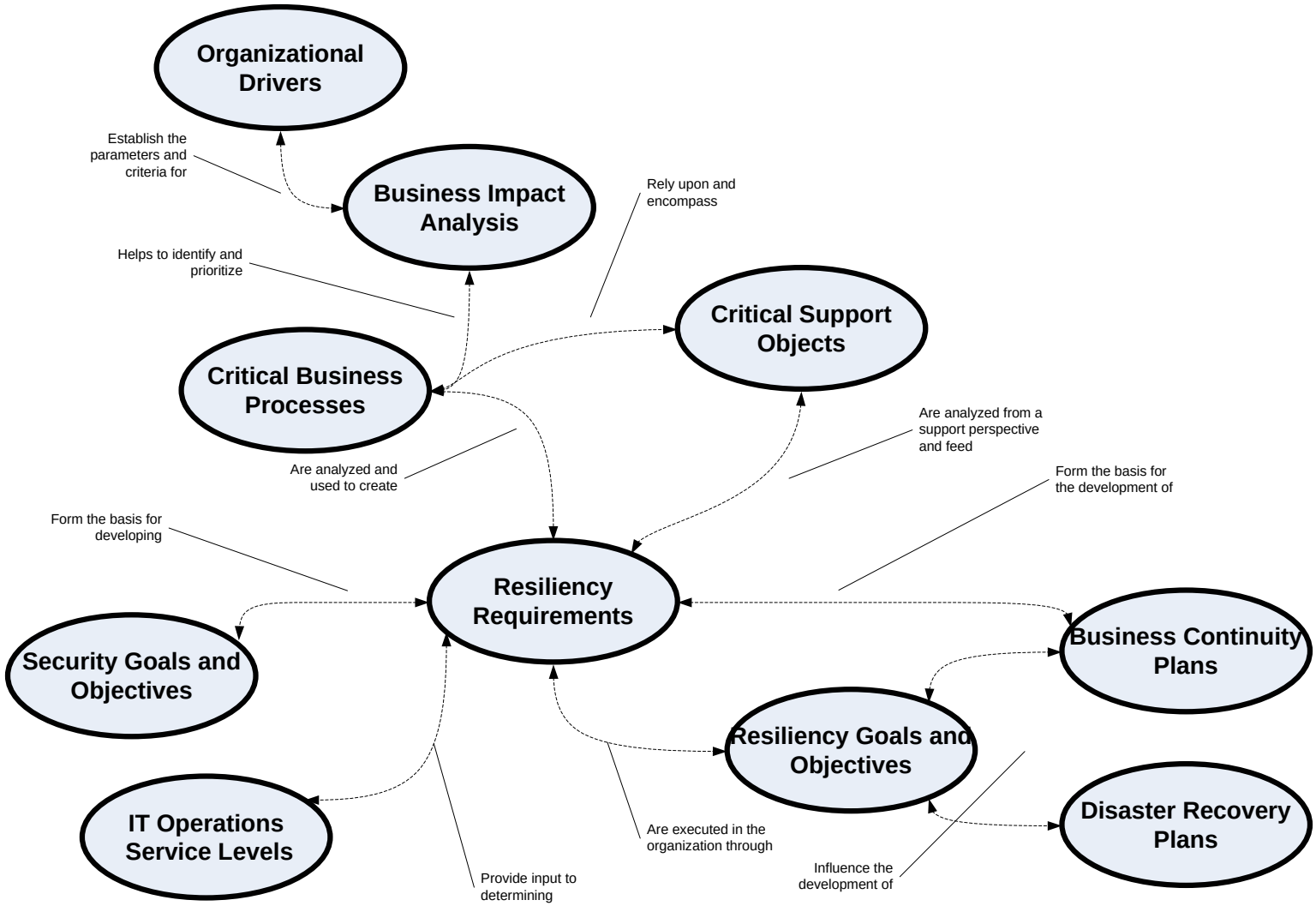
Requires enterprise collaboration and coordination

Convergence of operational risk-based activities across the enterprise with similar requirements



Common purpose: achieve and sustain a state of adequate enterprise resiliency

Requires an enterprise view



Resilient organizations. . .

Are agile and prepared

Inculcate risk management as a way of life

Endure disruptions to primary earnings drivers

Change before they need to

Sense, respond, thrive, *and improve*

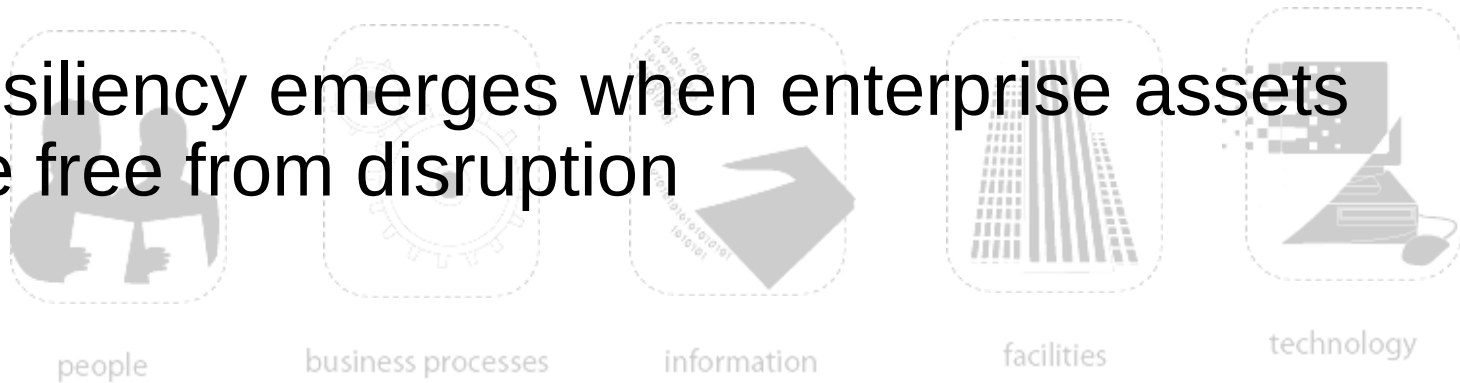
Use security as a means to control, manage, and enable resiliency

Positioning security in resiliency

Security is an operational risk management activity → Managing operational risk contributes to operational resiliency

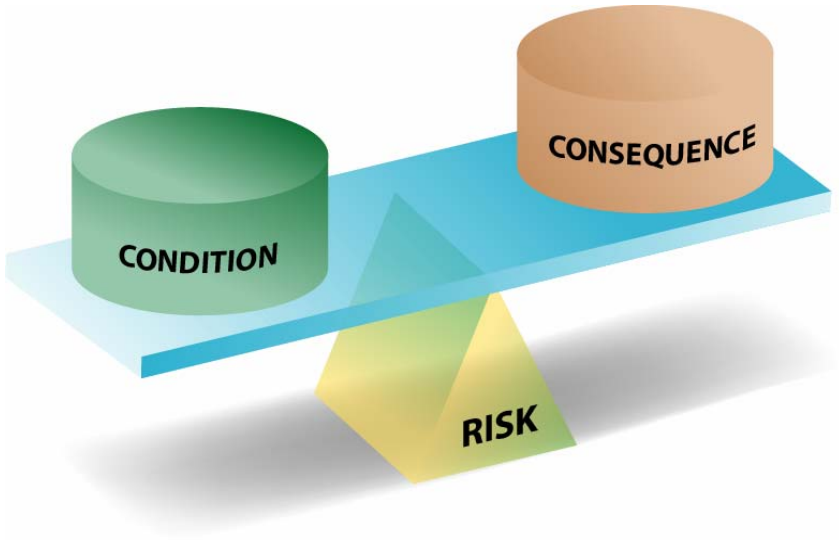
Security is focused on enterprise assets → Operational resiliency depends on the resiliency of enterprise assets

Resiliency emerges when enterprise assets are free from disruption



Security is a resiliency activity

- Managing firewall rule-sets
- Installing access controls to facilities
- Limiting access to intellectual property or confidential information
- Developing business continuity and disaster recovery plan



The aim of these "security" activities is ultimately to manage operational risk and resiliency.

Recasting security in resiliency

How do we perform security as an enabler to resiliency?

From

- **Managing to threat and vulnerability**
- **No articulation of desired state or goals**
- **Possible security overkill or misapplied security activities**

To

- **Managing to threat and IMPACT**
- **Adequate security and resiliency defined as desired state**
- **Security in sufficient balance to cost and risk**

Resiliency expands security

Allows operational risk to be considered alongside organization's traditional risk management activities

Moves the focus of security from point solutions (best practices) to a process-oriented approach

Integrates security into the overall corporate strategy

Positions security as a means to an end

Focus on Resiliency: A Process-Oriented Approach

Back to basics

To make security a more effective activity in the organization, we must:

1. Re-define its role and contributions
2. Acknowledge risk as the driver
3. Position it as an enabler to resiliency
4. Manage it as a process that can be improved: PLAN→DO→CHECK→ACT

What is a process?

A series of actions, changes, or functions bringing about an intended or expected result.

- The process of digestion
- The process of evolution
- The process of paying vendors
- The process for signing up for benefits
- The process of managing enterprise resiliency

The American Heritage® Dictionary of the English Language, Fourth Edition
Copyright © 2000 by Houghton Mifflin Company.

A process approach -1

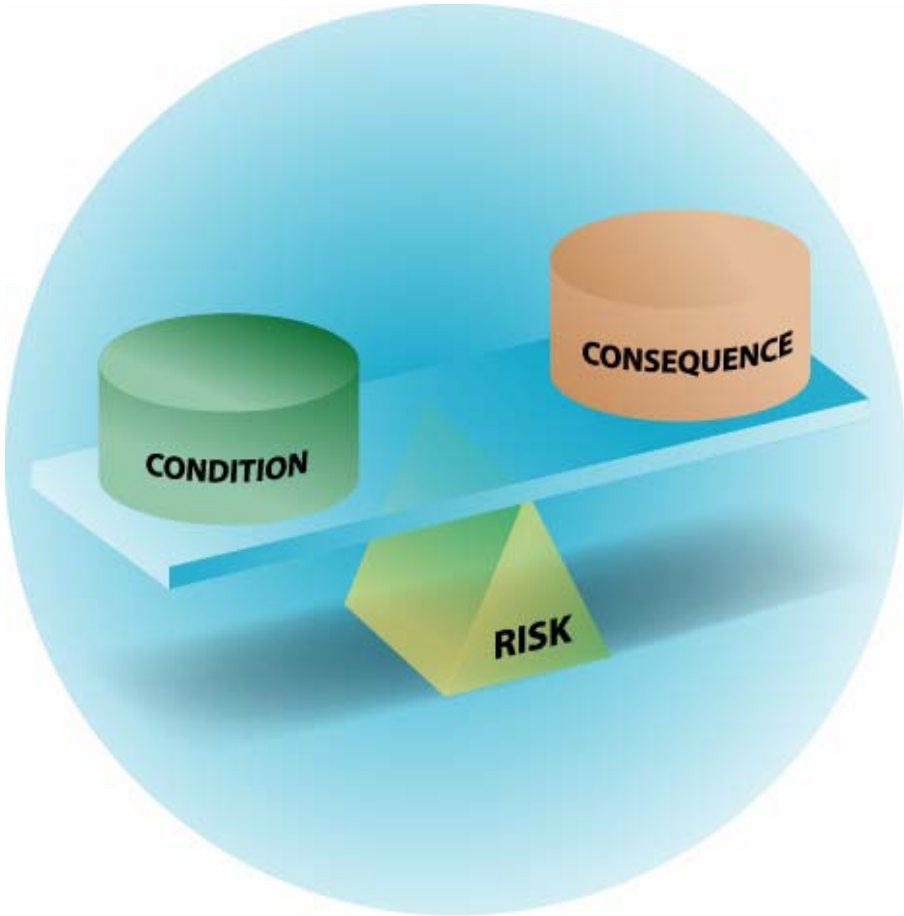
Elevating the management and coordination of all risk-based activities to the enterprise level.

- Setting and achieving common goals
- Collaborating and sharing resources
- Eliminating stovepipes
- Eliminating redundancy
- Measuring effectiveness
- Systematically improving

Working smarter, not harder

A process approach -2

- Managing both sides of the risk equation from an enterprise perspective
- Managing across all risk-based activities
- Taking a holistic view
- Performing security in context



Getting “resiliency” to emerge

CERT

Process improvement

Activity of elevating the performance of a process with regard to its goals

Processes can be measured and actively managed

Gaps in expected performance can be identified, prioritized, and corrected

What is learned can be fed back into the process for continuous improvement and maturity

Common frameworks

There are process improvement frameworks for various disciplines and industries

Aimed at defining and improving processes in the context of the enterprise

- Capability Maturity Model(s) for software and systems engineering
- Six Sigma
- Goal, Question, Metric (GQM)
- ISO9000
- TQM
- Toyota Production System/Lean Manufacturing

Viewing security as a process

A process-view brings process improvement constructs to security and resiliency

Common goals replace functional goals

Common resiliency requirements drive all risk-based activities

Efficiencies are realized in the collaboration and coordination of efforts and assets

Stovepipes are reduced, perhaps eliminated

Process vs. best practices

Processes define **what** you do and are relatively stable over time

Practices define **how** you do it, which changes over time

Aiming at the process level means active management and goal achievement

Practices are a means to enabling processes

Focus on Resiliency: Thinking About Solutions

Embracing process improvement -1

Security-resiliency link is explicit

Traverses the entire organization

Goals are organization-driven and dynamic, and *specific*

Security practices alone cannot keep up

Improvement in meeting security and resiliency goals is dependent on active management of the process

Embracing process improvement -2

Process management brings active awareness of security-resiliency link

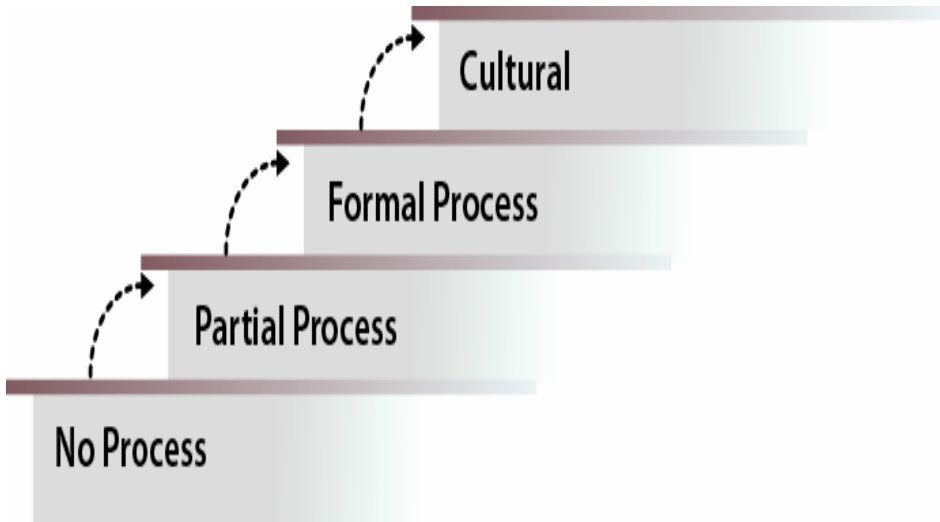
Process maturity brings increasing capability for meeting goals and sustaining the process

Process approach helps to guide the selection and implementation of practices

“Are we secure?” is answered in the context of capability, not threat or incident – success more predictable?

How mature are you?

Most organizations have some rudimentary process (implicit or explicit) for security management, but it may not be effective for meeting goals.



Thanks to www.betterproductdesign.net/maturity.htm for the generic categories.

Lack of process

No process defined or performed

Anarchy and heroics

No awareness of benefits of process-orientation

AD-HOC

Common attributes:

- Focus on events
- Ambiguous lines of responsibility
- Funding sporadic
- No alignment to strategic drivers
- Highly dependent on people
- No governance structure

Partial process

Process recognized

Still functionally focused (not enterprise-wide)

Not repeatable or actively managed

VULNERABILITY-DRIVEN

Common attributes:

- Focus on vulnerabilities
- Responsibility emanates from IT
- Considered an expense or burden
- Awareness of strategic drivers
- Still dependent on people and vul catalogs
- Informal governance

Formal process

Performed and managed

Repeatable

Spans enterprise

Not completely ingrained in culture

RISK-DRIVEN

Common attributes:

- Focus on critical assets
- Responsibility of key organizational managers and IT
- Funded as an expense
- Implicit alignment to strategic drivers
- Dependent on localized risk management
- Informal governance, possibly CRM

Cultural

Performed and managed

Repeatable and proactive

Spans and involves enterprise

Process continually measured and improving

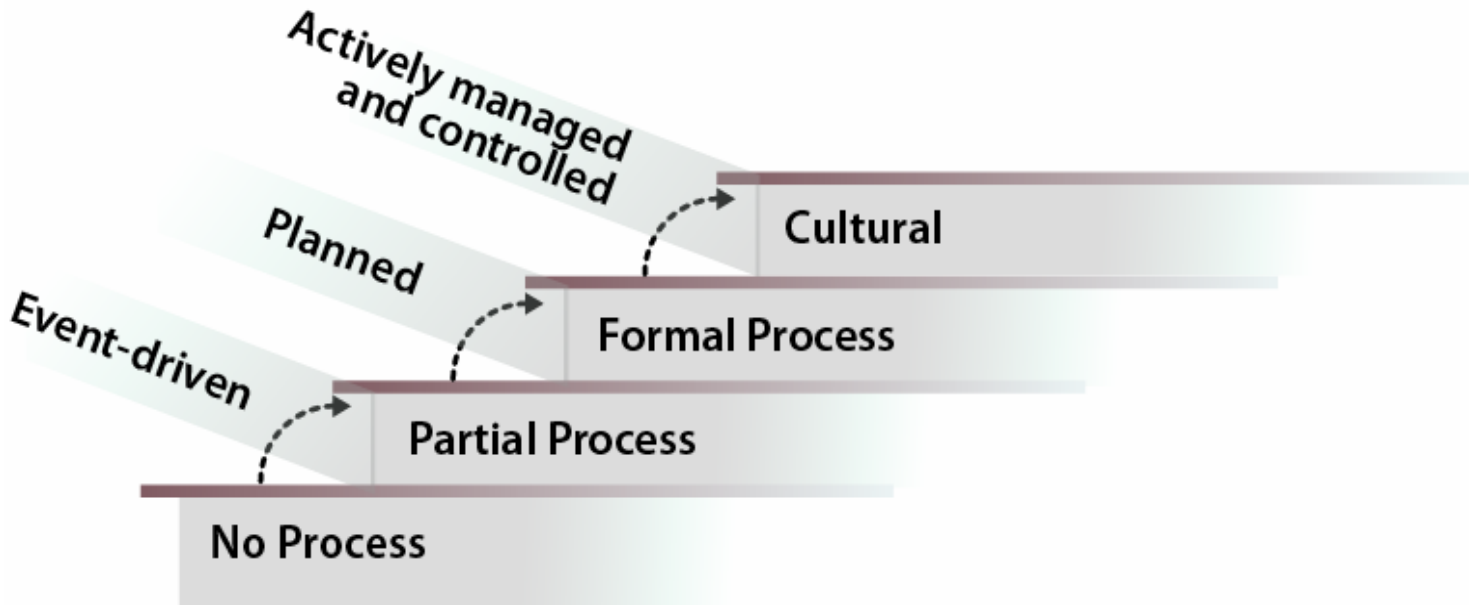
Fundamental to organizational success

ENTERPRISE-DRIVEN

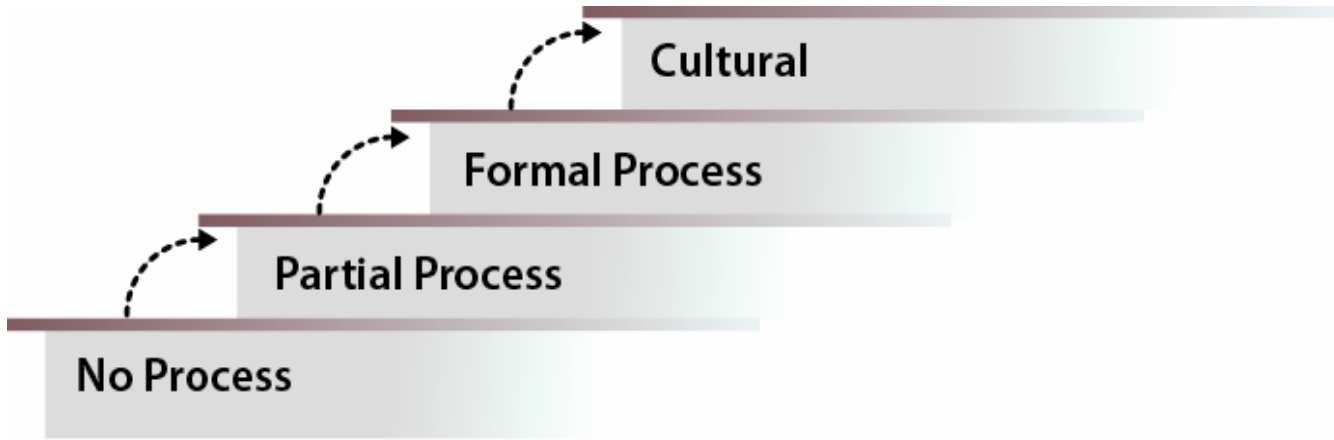
Common attributes:

- Focus on critical assets, processes, strategic drivers
- Responsibility of high-level executive
- Capitalized
- Explicit alignment to strategic drivers
- Reliant upon enterprise capabilities
- Formal governance and feedback

Increasing levels of competency



Improving the security discipline

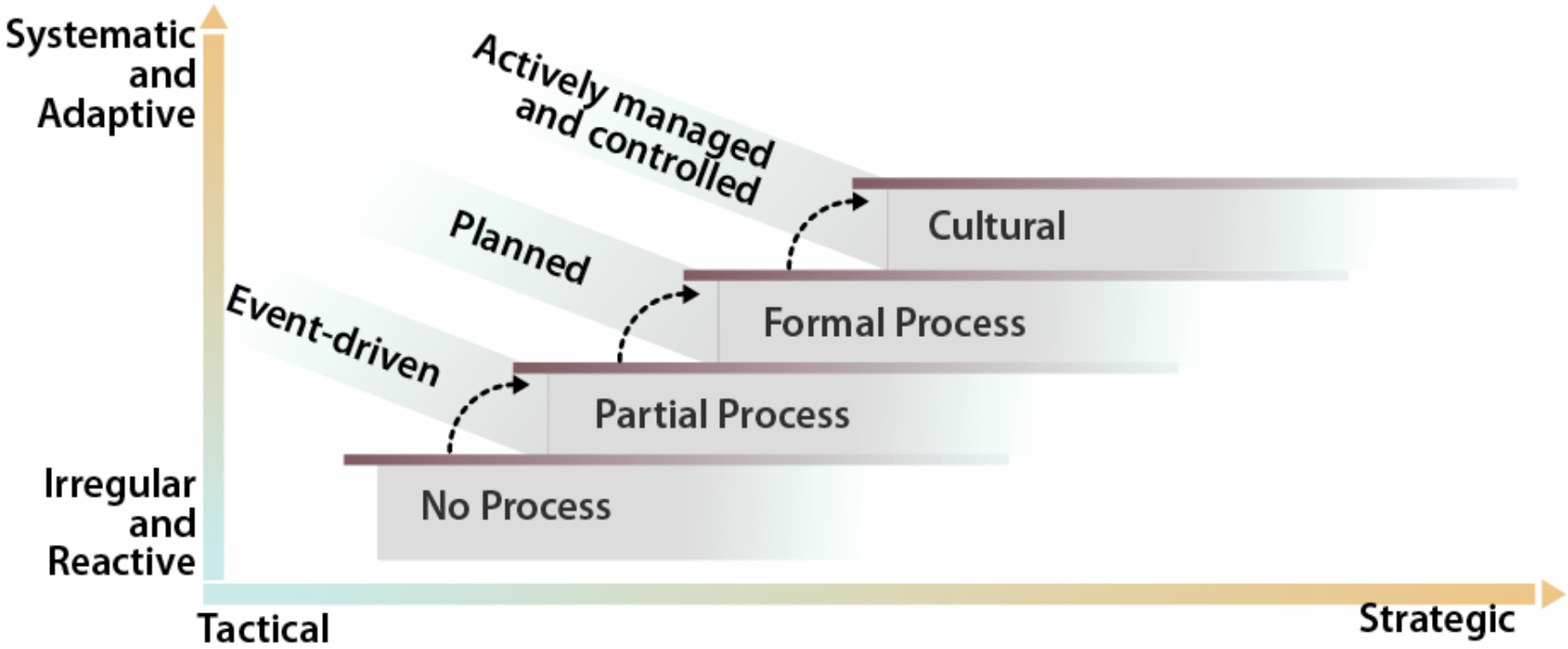


- Technical problem
- Owned by IT
- Expense-driven
- Practice-centric
- Security and survivability

→

- Business problem
- Owned by organization
- Investment-driven
- Process-centric
- Enterprise resiliency

Toward continuous improvement



What are we doing?

PrISM – Process Improvement for Security Management

- A framework for describing the security process
- Described as a set of enterprise capabilities that collectively define the process
- Defining a roadmap for process measurement and improvement
- Linked to common practices and activities
- *Descriptive*, not prescriptive

Developing PrISM

Affinity grouping of standards, guidelines, practices

Developing and defining capability areas

Determining institutionalizing features—collaboration between capability areas

- “products, activities, agents”

Exploring capability and maturity modeling characteristics

Practice mapping and analysis

What do current best practices tell us?

What capabilities do they represent?

Over 750 practices representing

- COBIT
- BS7799/ISO17799
- ITIL
- ISF
- NIST 800 series
- SEI BOK
- Various BC/DR

Organizations can use PrISM to

Understand the essential capabilities necessary to manage security effectively to achieve goals

Gauge their current level of capability

Determine the necessary level of capability given their organizational drivers

Develop a road map for process improvement to meet desired target

Improve selection and implementation of complimentary security practices to achieve goals

Improve regulatory compliance competencies

Capability areas

Capabilities cover the five resiliency objects.

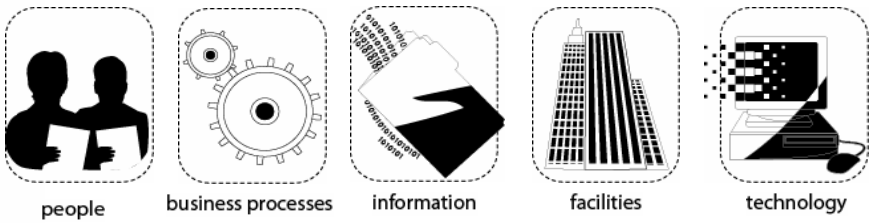
Capabilities traverse many organizational entities and functions.

- Enterprise
- People
- Technology assets and infrastructure
- Information and data
- Physical plant
- Resiliency relationships
- Resiliency delivery
- Sustaining resiliency

*To date, we have identified 42 candidate capabilities.

Enterprise

Sponsor, support, and promote an enterprise view and direction for resiliency.



- Enterprise Focus
- Strategic View
- Resiliency Governance
- Resiliency Standards and Policies
- Resiliency Planning
- Resiliency Requirements Management
- Risk Foundation for Resiliency
- Compliance Management
- Business Process Management
- Resiliency Resource Management

People

Enable the human resources of the organization to contribute to its resiliency.

people

- Workforce Competencies
- Resiliency Workforce Training
- Resiliency Workforce Management
- Human Resources Management
- Resiliency Awareness and Outreach

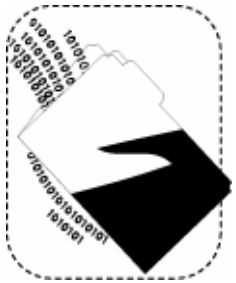
Technology assets and infrastructure

Ensure a reliable and stable infrastructure is available as needed to support critical business processes.

- Technology Asset Management
- IT Operational Resiliency
- Software and Systems Resiliency Management

Information and data

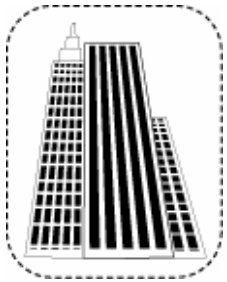
Protect and make available the critical information necessary for use by critical business processes.



- Information Asset Management

Physical plant

Ensure the physical structures of the organization are available to support critical business processes.



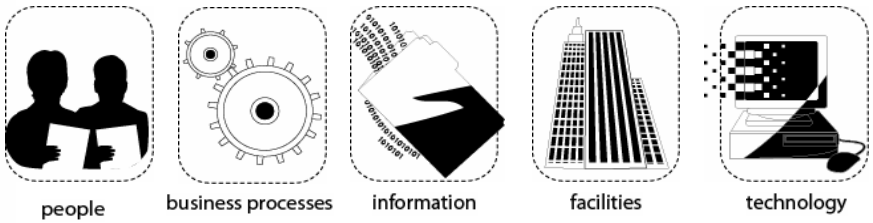
facilities

- Resiliency Facility Management
- Enterprise Facilities Management

Resiliency relationship management

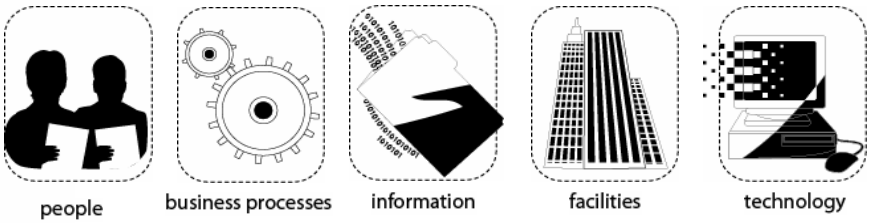
Actively manage the "resiliency value chain" of the organization to ensure upstream and downstream contributions to the organization's resiliency.

- Internal Partnerships
- Business Partnership Management
- Stakeholder Relationship Management
- Resiliency Partner Management
- Public Authority Relationship Management
- Contract Management



Resiliency delivery

Identify and deliver resiliency services based on organization-driven resiliency requirements.

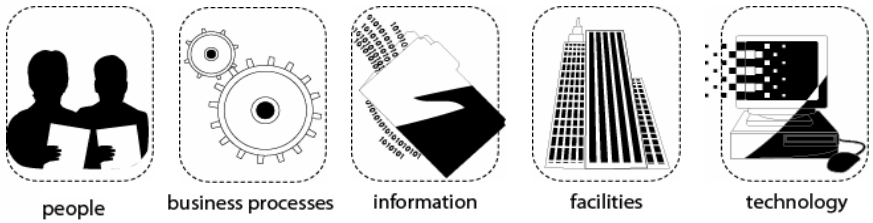


- Resiliency Support Technology
- Continuity Planning
- Continuity Planning Validation
- Recovery Planning
- Restoration Planning
- Communications
- Event Identification and Analysis
- Crisis Management

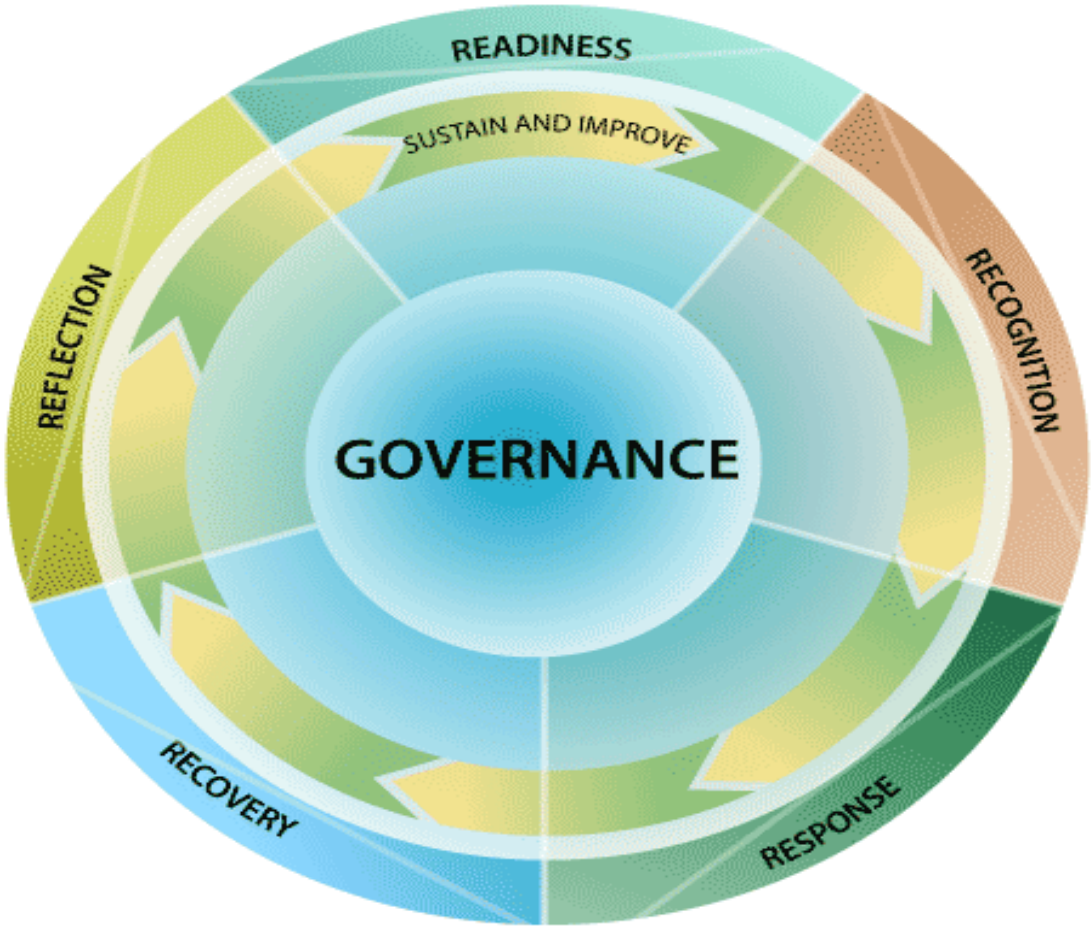
Sustaining resiliency

Manage the resiliency process enterprise-wide to ensure continuous improvement and alignment with organizational drivers.

- Inter-group Coordination
- Resiliency Process Management
- Quality Assurance
- Resiliency Services Definition
- Resiliency Service Delivery
- Auditing and Monitoring



Represent a broad range of activities



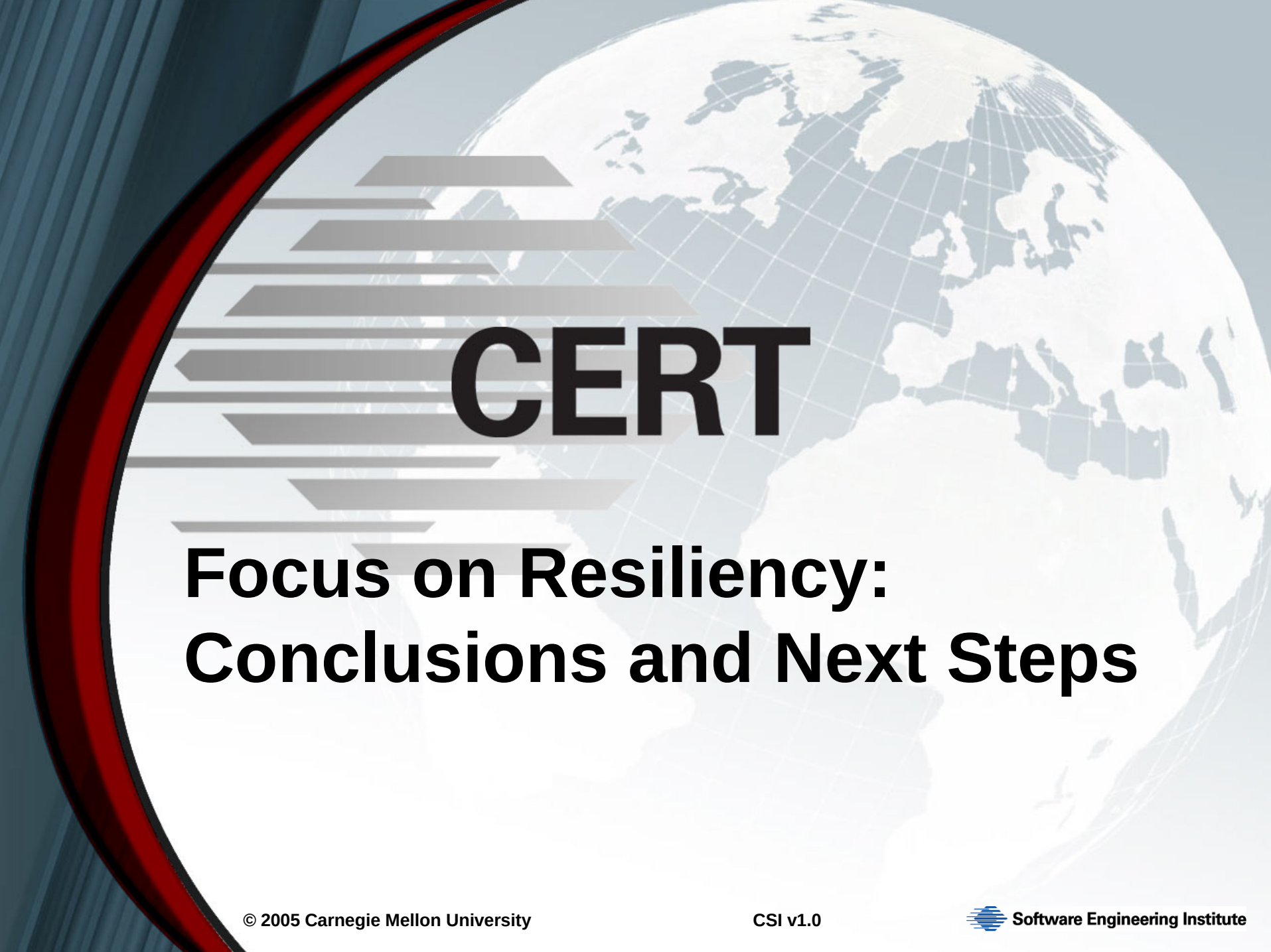
From PrISM to Maturity Model?

Process maturity concepts are integral to solving current security management challenges

Focus on security *management* process; **not** a means for rating how secure an organization is

Aim is process improvement to meet goals more consistently and predictably

Community calling for a model; lacks experience



Focus on Resiliency: Conclusions and Next Steps

Conclusions

Focusing on resiliency properly focuses security activities in an enterprise context

Security and resiliency are enterprise spanning processes for managing the risk equation

An enterprise enhances its ability to meet its security and resiliency goals by improving how it manage these processes

Collaborating with industry

Recent collaboration with Financial Services Technology Consortium

Advancing concepts of resiliency and security process management through the financial services industry

“Resiliency Maturity Model” project

More information: www.fstc.org

On the horizon

Expansion of PrISM concepts/underlying principles

Completion of v1.0 of PrISM Framework and technical report

Development/deployment of framework questionnaire

Development of notional metrics to measure success and improvement

Continued exploration of security-maturity connection

Continued research into resiliency-ESM connection

Parting thoughts

Security is not a one-shot activity.

Security is not only about technology.

Security lives in an organizational and operational context.

Security is a collaborative effort that must draw on a broad array of organizational capabilities.

Security strategies must be aligned with the organization's strategic drivers and business objectives.

Risk assessment and risk management must drive decision-making.

In the long run, security is about enhancing and sustaining the organization's *resiliency*.

Contact Us

Contact Information

Speakers
Richard Caralli
e-mail: **rcaralli@cert.org**

James Stevens
e-mail: **jfs@cert.org**

Phone
412-268-5800
(8:30 a.m. - 4:30 p.m. EST)

Web
http://www.cert.org
http://www.cert.org/nav/index_green.html

Postal Mail
Software Engineering Institute
ATTN: Customer Relations
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Useful references

"The Quest for Resilience" by Gary Hamel and Liisa Valinkangas, Harvard Business Review, September 2003

"Enterprise Resilience: Managing Risk in the Networked Economy" by Randy Starr, Jim Newfrock, and Michael Delurey, strategy + business Reader, issue 30, Booz-Allen